BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Fault detection method

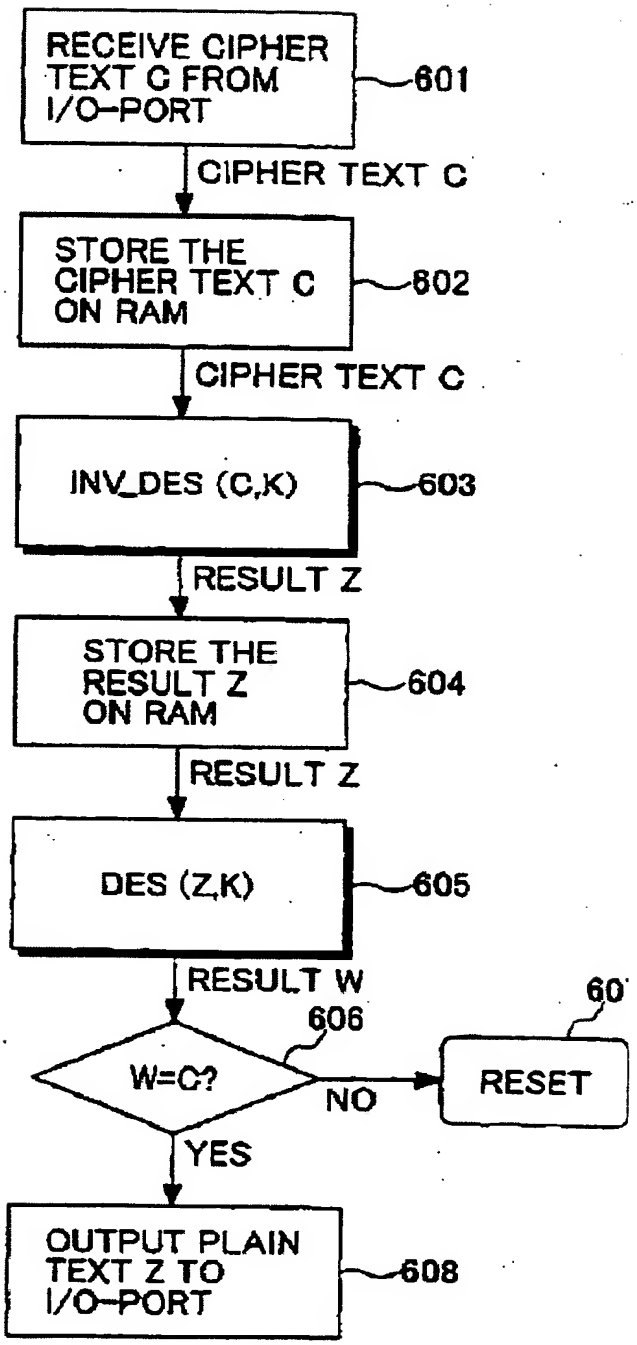
Patent number: US2002124179
Publication date: 2002-09-05
Inventor: KAMINAGA MASAHIRO (JP); OHKI MASARU (JP); ENDO TAKASHI (JP); WATANABE TAKASHI (JP)
Applicant: HITACHI LTD (US)
Classification:
- international: H04L9/00
- european: H04L9/06C, H04L9/30F
Application number: US20010931937 20010820
Priority number(s): JP20010058087 20010302

Also published as:
EP1237322 (A2)
JP2002261751 (A
EP1237322 (A3)

Abstract not available for US2002124179
Abstract of correspondent: **EP1237322**

The disclosed techniques are as shown below. The subject of the invention is to provide a crypto-processing method capable to confront an attack, which intentionally causes an erroneous operation and takes out secret information to be done against a device which performs a crypto-processing inside the device such as an IC card. The solution means for such an attack is shown below. A ciphertext C is received through the I/O port on an IC card, etc. (step 601), the ciphertext C is stored on a RAM (step 602), a decryption process of the ciphertext C is performed (step 603), and the processing result Z is stored on a RAM (step 604). For the processing result Z, an encryption process is executed (step 605), and the processing result W and the original plaintext C are compared with each other (step 606). When the processing result W coincides with the original plaintext C, the plaintext Z is output to the I/O port (step 608), and if not, a reset is effected (step 607).

FIG.6



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－261751
（P2002－261751A）
(43)公開日　平成14年９月13日(2002.9.13)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/10		Ｇ０９Ｃ　1/00	６１０Ｚ	５Ｂ０３５
Ｇ０６Ｋ　19/07			６２０Ｚ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６１０		６６０Ａ	
	６２０	Ｈ０４Ｌ　9/00	６２１Ａ	
	６６０	Ｇ０６Ｋ　19/00	Ｎ	

審査請求　未請求　請求項の数12　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－58087(P2001－58087)

(22)出願日　平成13年３月２日(2001.3.2)

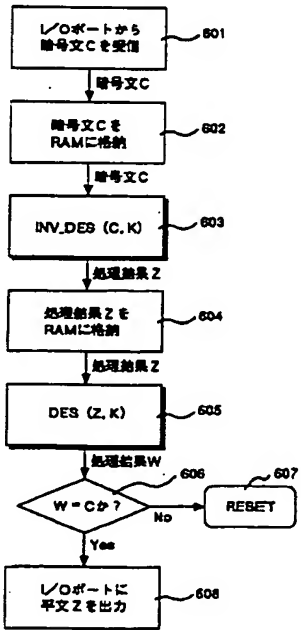
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　神永　正博
東京都国分寺市東恋ヶ窪一丁目280番地
株式会社日立製作所中央研究所内
(72)発明者　遠藤　隆
東京都国分寺市東恋ヶ窪一丁目280番地
株式会社日立製作所中央研究所内
(74)代理人　100068504
弁理士　小川　勝男　（外２名）

最終頁に続く

(54)【発明の名称】　暗号処理方法

(57)【要約】
【課題】ＩＣカードなど内部で暗号処理を行なう装置に対して故意にエラーを引き起こし、秘密情報を取り出すような攻撃に対抗する暗号処理方法を提供する。
【解決手段】ＩＣカードなどのＩ／Ｏポートから暗号文Ｃを受信し（ステップ601）、この暗号文ＣをＲＡＭに格納し（ステップ602）、暗号文Ｃに対して復号化処理を行ない（ステップ603）、その処理結果ＺをＲＡＭに格納する（ステップ604）。処理結果Ｚに対して暗号化処理を行ない（ステップ605）、その処理結果Ｗと元の暗号文Ｃとを比較して（ステップ606）、一致すればＩ／Ｏポートに平文Ｚを出力する（ステップ608）。両者が不一致であればリセットする（ステップ607）。

図 6



【特許請求の範囲】

【請求項1】情報処理装置を利用して対称鍵暗号化処理を行なう方法であって、（１）入力される平文Mに秘密鍵Kを適用する暗号化処理Z＝E（M，K）を行なってその結果Zをメモリに格納し、（２）前記メモリ上の結果Zに対して復号化処理W＝D（Z，K）を行なってその結果Wをメモリ上に格納し、（３）前記の処理結果Wと平文Mとが一致している場合には、処理結果Zを出力し、（４）前記の処理結果Wと平文Mとが不一致の場合には、処理結果の出力を抑止することを特徴とする暗号処理方法。

【請求項2】前記暗号化処理及び復号化処理をＤＥＳ(Data Encryption Standard)に従って実行することを特徴とする請求項1記載の暗号処理方法。

【請求項3】前記処理結果の出力を抑止する方法として、前記情報処理装置をリセットすることを特徴とする請求項1記載の暗号処理方法。

【請求項4】前記情報処理装置及び前記メモリは、ＩＣカード上に搭載されるそれぞれ演算装置及び記憶装置であることを特徴とする請求項1記載の暗号処理方法。

【請求項5】情報処理装置を利用して対称鍵復号化処理を行なう方法であって、（１）入力される暗号文Cに秘密鍵Kを適用する復号化処理Z＝D（C，K）を行なってその結果Zをメモリに格納し、（２）前記メモリ上の結果Zに対して暗号化処理W＝E（Z，K）を行なってその結果Wをメモリ上に格納し、（３）前記の処理結果Wと暗号文Cとが一致している場合には、処理結果Zを出力し、（４）前記の処理結果Wと暗号文Cとが不一致の場合には、処理結果の出力を抑止することを特徴とする暗号処理方法。

【請求項6】前記暗号化処理及び復号化処理をＤＥＳ(Data Encryption Standard)に従って実行することを特徴とする請求項5記載の暗号処理方法。

【請求項7】前記処理結果の出力を抑止する方法として、前記情報処理装置をリセットすることを特徴とする請求項5記載の暗号処理方法。

【請求項8】前記情報処理装置及び前記メモリは、ＩＣカード上に搭載されるそれぞれ演算装置及び記憶装置であることを特徴とする請求項5記載の暗号処理方法。

【請求項9】情報処理装置を利用して非対称鍵復号化処理を行なう方法であって、（１）入力される暗号文Cに秘密鍵X，公開鍵情報J を適用する復号化処理Z＝D（C，X，J）を行なってその結果Zをメモリに格納し、（２）前記メモリ上の結果Zに対して暗号化処理W＝E（Z，J）を行なってその結果Wをメモリ上に格納し、（３）前記の処理結果Wと暗号文Cとが一致している場合には、処理結果Zを出力し、（４）前記の処理結果Wと暗号文Cとが不一致の場合には、処理結果の出力を抑止することを特徴とする暗号処理方法。

【請求項10】前記暗号化処理及び復号化処理をＲＳＡ暗号化方式に従って実行することを特徴とする請求項9記載の暗号処理方法。

【請求項11】前記処理結果の出力を抑止する方法として、前記情報処理装置をリセットすることを特徴とする請求項9記載の暗号処理方法。

【請求項12】前記情報処理装置及び前記メモリは、ＩＣカード上に搭載されるそれぞれ演算装置及び記憶装置であることを特徴とする請求項9記載の暗号処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、高いセキュリティを持つＩＣカードなどの耐タンパー暗号処理方法に関するものである。

【０００２】

【従来の技術】ＩＣカードは、勝手に書き換えることが許されないような個人情報の保持や、秘密情報である暗号鍵を用いたデータの暗号化や暗号文の復号化を行う装置である。ＩＣカード自体は電源を持っておらず、ＩＣカード用のリーダライタに差し込まれると、電源の供給を受け、動作可能となる。動作可能になると、リーダライタから送信されるコマンドを受信し、そのコマンドに従ってデータの転送等の処理を行う。ＩＣカードの一般的な解説は、オーム社出版電子情報通信学会編水沢順一著「ＩＣカード」などにある。

【０００３】ＩＣカードの構成は、図1に示すように、カード101の上に、ＩＣカード用チップ102を搭載したものである。図に示すように、一般にＩＣカードは、ISO7816の規格に定められた位置に供給電圧端子Vcc、グランド端子GND、リセット端子RST、入出力端子I/O及びクロック端子CLKを持ち、これらの端子を通してリーダーライタから電源の供給やリーダライタとのデータの通信を行う(W.Rankl and Effing : SMARTCARD HANDBOOK、John Wiley & Sons、1997、pp.41参照)。

【０００４】ＩＣカード用チップの構成は、基本的には通常のマイクロコンピュータと同じ構成である。その構成は、図2に示すように、中央処理装置(ＣＰＵ)201、記憶装置204、入出力（Ｉ／Ｏ）ポート207、コ・プロセッサ202からなる（コ・プロセッサはない場合もある）。ＣＰＵ201は、論理演算や算術演算などを行う装置であり、記憶装置204は、プログラムやデータを格納する装置である。入出力ポートは、リーダライタと通信を行う装置である。コ・プロセッサは、暗号処理そのもの、または、暗号処理に必要な演算を高速に行う装置であり、例えばＲＳＡ暗号の剰余演算を行うための特別な演算装置や、ＤＥＳ暗号のラウンド処理を行う暗号装置などがある。ＩＣカード用プロセッサの中には、コ・プロセッサを持たないものも多くある。データバス203は、各装置を接続するバスである。

【０００５】記憶装置２０４は、ＲＯＭ(Read Only Memory)やＲＡＭ(Random Access Memory)、ＥＥＰＲＯＭ(E

プ内に格納されている秘密鍵Kを用いて、通常のＤＥＳの操作を行ない、平文Z = INV_DES(C, K)を求める。ＤＥＳは、16ラウンドからなる攪拌操作列であり、攪拌操作は、転字と換字から構成されている。このＤＥＳの攪拌操作を逆に遡る操作を行なうことにより、逆変換DESを構成することができる。従って、正しく復号処理INV_DES(C, K)が行われれていれば、DES(Z, K) = Cが成り立たなければならないはずである。そこでDES(Z, K)の処理結果WをＲＡＭ等に格納して後、WとCを比較し、W = CとなればZは正しい処理結果であることがわかるので、これを正しい処理結果として出力し、WがCと異なれば、出力しない。逆に平文を暗号化する場合は、復号化して確認することができることは言うまでもない。

【００１６】一方、非対称鍵暗号の場合、例えば、ＲＳＡ暗号を例に取ると、ＩＣカードでは、（暗号化に用いられる公開鍵指数eは、通常、3又は、65537である）公開鍵指数e、公開モジュラスNを用いて、平文Mに対して、C = RSA(M, (e,N)) = M^e mod Nを計算して、これを暗号文とする。この暗号文Cは、公開鍵情報J=(e,N)の持ち主によってＩＣカードにて受信され、このＩＣカードに保持されている秘密鍵指数xを用いて、INV_RSA(C, x, J) = C^x mod N = Mという操作で復号され、処理結果zを得る。一般にＩＣカードのセキュリティにおいては、カードチップ内に格納されている秘密鍵指数xがアタックターゲットであり、この復号化処理において誤作動が生ずると、xに関する情報がカード外にリークする。これを守るために、計算結果Zをすぐに出力せず、ＲＡＭ等に格納し、暗号化処理結果wとcを比較し、w = cであれば、Zは正しい処理結果であることがわかるので、これを正しい処理結果として出力し、wがcと異なれば、出力しない。

【００１７】以上を勘案すると、本発明の趣旨は、暗号化または復号化の操作に対し、その逆操作、すなわち暗号化に対しては復号化、復号化に対しては、暗号化の操作を行なって、元の結果が得られるかどうかを確認することにある。従って、暗号の種類が、ＤＥＳであるか、ＲＳＡであるかと言った問題は本質的ではない。つまり、上記2種類の暗号以外に、他の秘密鍵暗号、公開鍵暗号に対しても同様の操作ー逆操作というプロセスで誤作動検出を行なうことができる。

【００１８】

【発明の実施形態】本実施例では、秘密鍵暗号の代表例であるＤＥＳ暗号を例に取る。ここでは、秘密鍵暗号の代表例としてＤＥＳを例として採用するのみであって、ＤＥＳ以外の秘密鍵暗号においても同様に本発明を適用することができる。

【００１９】図3は、ＤＥＳの基本構造を示す図である。ＤＥＳは、64ビットの平文を64ビットの鍵K（但し、このうち8ビットをパリティビットとして用いるので、実質の鍵長は、56ビットである）をビット置換302, 304によって変形し、第一段目の部分鍵K1を生成し、置換302を行なった鍵ビットを左巡回シフト306,307で半々のビット毎に変形し、これをビット置換304と同じビット置換（PC-2）を施して部分鍵K2を生成する。これを繰り返し、最終的に、第16段目でも同様に左巡回シフト309,310で半々のビット毎に変形し、これをビット置換304と同じビット置換311を施して部分鍵K16を生成する。一方、平文は、初期置換IP301を施した後に、64ビットを32ビットずつに左右に分離される。この右半分を部分鍵K1と共にf関数303と呼ばれる非線型の変換に代入し、その結果と左半分のビットとビット毎の排他的論理和305を取って、第2ラウンドの右半分の32ビットとし、先の初期置換301の出力の右半分を第2ラウンドの左32ビットとして、以下同様の操作を繰り返し、最終的に第15ラウンド目の出力を部分鍵K16を用いて変形し、左右入れ替えた後、初期置換IPの逆置換313に代入して、その結果を64ビットの暗号文として出力する。

【００２０】この復号変換INV_DESは、図4のように構成することができる。図3との違いは、第16ラウンド目の処理から始めるということである。そのため先に左巡回シフト306,307,309,310で変形した部分を、逆に右巡回シフト406,407,409,410する。部分鍵はK16, K15, ...,K1というように暗号化変換とは逆に用いる。この操作は、ちょうど図3の処理を全て逆方向に行なうということに他ならない。

【００２１】いま例えば、暗号化変換で、第16ラウンド目で、特定の処理ビットがエラーにより反転したとする。このとき、第16ラウンド目に使用されている部分鍵K16が何であるかによって、反転した際の処理結果が変化する。反転した処理結果とK16の関係を詳細に調べると、両者の間に数学的関係が現れる。これを複数の入力に対して連立して解くことにより、K16の候補を大幅に減らすことができる。K16が特定できれば、ＤＥＳの鍵Kを決定するには、残りの8ビットを決定すればよいので、高々2^8 = 256通りを試せば、正しい解を決定することができる。

【００２２】ＤＥＳ暗号に対して誤作動を起こして解析する手法は、極めて複雑であるので、ここでは要点のみ示した。詳細は、国際会議CRYPTO'97にて発表された論文Eli Biham, Adi Shamir: “Differential Fault Analysis of Secret Key Cryptosystems”, Springer-Verlag LNCS1294, pp513-525に書かれている。

【００２３】このような攻撃を行なうには、アタッカーは、暗号化（または復号化）の結果を解析する必要がある。鍵K、平文Mに対する暗号化結果Zは通常ＲＡＭに一時的に格納され、ＩＣカードのＩ／Ｏ端子を通して出力される。アタッカーは、暗号化処理中に異常電圧、異常クロック、異常電磁波などを印加し、エラーを引き起こす。従ってエラー注入が成功した場合のZは、一般に正しい処理結果DES(M, K)ではない別の値になっているは

【００３１】また本発明の考え方は、暗号化処理、復号化処理の一部にも適用することができる場合がある。例えば、置換処理の最中にエラーが生じたかどうかを判定するために、この置換処理の逆置換処理を行なって、誤作動を検出することも可能である。

【００３２】次に、非対称鍵暗号の場合について説明する。非対称鍵暗号に対する誤作動を利用したアタックのうち、最も有名なのは、ＣＲＴ（中国人剰余定理）を用いたＲＳＡ暗号処理に対するアタックである。この詳細はA.K.Lenstra氏のショートメモ“Memo on RSA Signature Generalization in the Presence of Faults”,1999に記載されているが、ここでは、このアタックについて、その原理を説明し、理解の助けとする。ＲＳＡ暗号および、ＣＲＴについては、岡本栄司著「暗号理論入門」（共立出版）や、A.J.Menezes, P.C. van Oorschot, S. A.Vanstone著 Handbook of Applied Cryptography,（CRC-Press）などに詳しく記載されている。

【００３３】簡単にＲＳＡ暗号を説明する。ＲＳＡ暗号では、大きな素数、例えば512ビットの2つの素数p,qの積 N = pq と Nと互いに素な数 e（ＩＣカードでは、3や、65537が用いられることが多い）をとり、これを公開鍵として公開鍵簿に登録する。このとき、この公開鍵の持ち主Aに送信者Bは、1以上N-1以下の数で表現されたデータ（平文） Mを、

y = M^e mod N

として暗号化して送信する。ここで、M^eはMのe乗を表す記号とする。この暗号文Ｒを受け取ったAは、xe mod (p-1)(q-1) = 1となる秘密鍵 x を用いて

y^x mod N

を計算する。ここで、(p-1)(q-1)は、Nのオイラー関数の値f(N)である。これは、Nと互いに素な自然数の個数に等しい。オイラーの定理によれば、

y^((p-1)(q-1)) mod N = 1

が成り立つ。一方、xe = 1 + k(p-1)(q-1)（kは整数）と書くことができるので、

y^x mod N
= (M^e)^x mod N
= M^(ex) mod N
= M^(1+k(p-1)(q-1)) mod N
= M*M^(k(p-1)(q-1)) mod N
= M

が成り立つ。従って、y^x mod Nを計算することによって、持ち主Aは、送信者Bの平文 M を復号することができる。この際、秘密鍵 x を計算するのに、Nの素因数 p, q が用いられている。現在のところ、素因数分解を介さないで、xを計算する方法は知られておらず、大きな素数の積を因数分解することは、現実的でない時間が必要であるので、Nを公開してもAの秘密鍵は安全である。

【００３４】ＩＣカードでは、公開鍵指数eとして、3や、65537が用いられることが多い。これは、暗号化の計算時間を短縮するという意味もあるが、eの値を知っても、直接的に秘密鍵指数x やNの素因数が危険に曝されることはないという事情によるものである。

【００３５】この計算法としては、アディション･チェイン方式などが採用される（上記「暗号理論入門」参照）ことが多いが、このようなアルゴリズムでは、処理が遅く、ＩＣカードを用いたトランザクションに要する時間がユーザの許容範囲を超えてしまう可能性がある。

【００３６】そこで、単純にx，Nに対するべき乗剰余計算を行なわずに、公開モジュラスNの二つの素因数p,qに対するべき乗剰余計算結果から、Mを導く方法が、ＣＲＴである。

【００３７】図9を用いて、ＣＲＴの処理を簡単に説明する。まず、計算に用いる値k=p^(-1) mod q, xp = x mod (p-1), xq = x mod (q-1)の値を計算する。普通、これらの値はＥＥＰＲＯＭに格納しておく。次にＩ／Ｏポートから暗号文yを受け取り（ステップ902）、この暗号文yを素因数p,qを法とする剰余yp = y mod p, yq =y mod qを求め、これをRAMに格納する（ステップ903）。次に、二つのべき乗剰余計算：

Cp = yp^xp mod p, Cq = yq^xq mod q

を行なう（ステップ904, 905）。次に、再結合計算：

S = (Cq - Cp)*k mod p
M = S*p + Cp

を行ない（ステップ906, 907）、Mを返す（ステップ908）。このMが、実際のy^xmod Nに一致する。

【００３８】この事実を数値的に確認しておく。暗号文 y = 79, N = 187(=11*17), x = 107とする。このx は、Nのオイラー関数値(11-1)*(17-1)=160に関して、e = 3の逆数になっている。このとき、実際の値は、

M = 79^107 mod 187
= 79^(5*3*7 + 2) mod 187
= 79^2 * (79^5 mod 187)^(3*7) mod 187
= 79^2 * 10^(3*7) mod 187
= 79^2 * (10^3 mod 187)^7 mod 187
= 79^2 * (65^7 mod 187) mod 187
= 79^2 * 142 mod 187
= 29

である。

【００３９】これをＣＲＴを用いて計算する。11*14 mod 17 = 1であるから、k = 11^(-1)mod 17 = 14であり、xp = 107 mod (11-1) = 7, xq = 107 mod (17-1) = 11である。また、yp = 79 mod 11 = 2, yq = 79 mod 17 = 11となる。

Cp = 2^7 mod 11 = 7
Cq = 11^11 mod 17 = 12

となるので、

S = (12 - 7)*14 mod 17 = 2
M = 2*11 + 7 = 29

= x^3 + ax + bまたは、
y^2 + xy = x^3 + ax + b
という標準形を持つ曲線である。（いずれの場合も、後に説明する無限遠点Oを含めて考える）。楕円曲線の形状は、図１１のようなものになる。本発明において、標数が2 であるか否かは、本質的ではないので、以下、簡単のため、標数が2 でない場合について説明する。また暗号で必要なのは、有限体の場合のみであるので、その場合に限って説明する。有限個の元からなる体を有限体またはガロア体といい、その構造はよく知られている。その最も単純な構成法は以下の通りである。

【００５２】まず、素数ｐを法とする整数環の剰余環Zp を考える。Zpにおいては、０以外の元は逆を持つので、体の構造を持っている。これを素体といい、Fpと書く。これが最も原始的な有限体の例である。

【００５３】次に、Fpの元を係数に持つ多項式f(X) を考え、その零点のうち、Fpに含まれないものをFpに添加することによって、新しい体を構成することができる。これを、Fpの有限次代数拡大体という。Fpの有限次代数拡大体の元の個数は、pのべきになっていることが知られている。その元の個数をqと書くとき、有限次代数拡大体をFqなどと表示することがある。

【００５４】楕円曲線上の点の間には、演算を定めることができる。図１２に示すように、楕円曲線上の二つの点、P,Qがあるとき、この二点を通る直線を引き（P=Qのときは接線を引く）、この直線が再び楕円曲線と交わる点Rをx 軸に関して対称に折り返した点は、曲線の対称性から、再び楕円曲線上の点となる。この点をP+Qと書き、PとQの「和」と定義する。交わる点がない場合は、架空の点として無限遠点というものを考え、この架空の点で交わっているものとみなす。無限遠点をOと書く。また、楕円曲線上の点Pとｘ軸に関して対称な位置にある点をPの逆元といい、-Pで表す。この「和」を用いて一点Pをk個加えたものを、kP、-Pをk個加えたものを-kPと書いて、Pのスカラー倍という。これらの座標は、P,Qの座標の有理式で表すことができ、従って、一般の体の上でこの演算を考えることができる。この「加法」は、通常の加法と同様に、結合法則、交換法則が成立し、この加法に関して、無限遠点Oは、通常の数での演算と同様にゼロの役割を果たし、-Pは、Pと加えると、Oになる。これは楕円曲線上の加法演算が、可換群（アーベル群）の構造を持つことを示している。これをモーデル-ヴェイユ群ということがある。楕円曲線E、定義体Fqを固定したときのモーデル-ヴェイユ群を、G(E/Fq)と書くことがある。G(E/Fq)の構造は非常に単純で、巡回群か、または二つの巡回群の直積と同型になることが知られている。

【００５５】一般に、kP=Qの値がわかっても、逆にk の値を知るのは計算量が膨大になるため、容易でない。これを楕円曲線上の離散対数問題という。楕円曲線暗号では、楕円曲線上の離散対数問題が困難であることに基づいている。

【００５６】楕円曲線を利用した暗号方式には種々のものがあるが、ここでは、特に楕円ＲＳＡ暗号方式を説明する。楕円ＲＳＡ暗号においては、環上で楕円曲線を取り扱う必要がある。環上での楕円曲線においても、形式的に有限体上での場合と同じ式を用いてモーデル-ヴェイユ群演算を行なうことができることが知られている。

【００５７】利用者は、二つの大きな素数p,q(p≡2 (mod 3), q≡2 (mod 3))を生成し、n=pq, m = lcm(p+1,q+1)を求める。適当なe∈Zm(=Z/mZ) , gcd(e,m)=1を定め、d =e^(-1) mod mを計算する。(e,n)が公開され、dまたは、p,qを秘密鍵とする。

【００５８】暗号化は次のように行なう。M = (Mx , My) ∈ Zn　Znを平文とする。環Zn上の楕円曲線を
E : y^2 = x^3 + b
として、楕円曲線上の点の加算を考えると、点の加算式は、b の値に依存しないことがわかる。そこで、b = My^2 - Mx^3 mod nとおく。すると、Mは、Ｅ上の点とみなすことができる。この設定上で、楕円曲線上の演算:
C = eM
を行なう。これが暗号化である。

【００５９】復号化は、
M = dC
とすればよい。この演算が復号になっていることは、ＲＳＡ暗号の場合と同様にして証明できるが、Eの位数がp+1になっていることを利用する必要がある。詳しくは、例えば、岡本龍明・山本博資「現代暗号」産業図書を参照されたい。

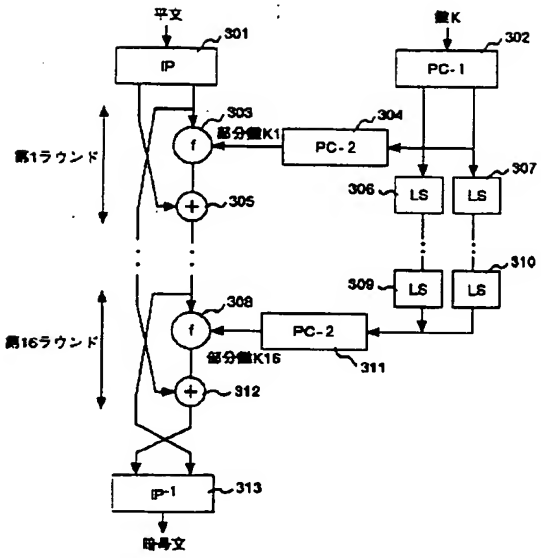
【００６０】上記の楕円ＲＳＡ暗号において、復号化操作におけるエラーを検出する方法について述べる。図１３に示すように、まず、Ｉ／Ｏポートより、公開鍵e,n及び暗号文Cを受信し（ステップ1301）、この暗号文CをＲＡＭに格納し（ステップ1302）、復号化計算（ステップ1303）にて、秘密鍵dを用いてdCを計算する。dCには、エラーが含まれている可能性がある。この処理結果をZとし、このZに対して、暗号化計算（ステップ1305）にて、W = eZを求める。もしも、Zが正しい結果であるならば、Wは、Cに等しくなければならない。そこで、W=Cであれば、このZをＩ／Ｏポートに出力し（ステップ1308）、W=Cでなければ、リセット（ステップ1307）を行なう。これは、本発明の実施例の一つである。

【００６１】以上に述べた処理方式は、抽象レベルでは、同一と考えられる処理を具現化したものであって、これらを、個々の暗号方式を超えて一般化することは自然なことである。

【００６２】以下、図１４を用いて上記エラー検出方法を抽象化したものを説明する。まず、Ｉ／Ｏポートより、公開鍵情報J及び暗号文Cを受信し（ステップ1401）、この暗号文CをＲＡＭに格納し（ステップ1402）、

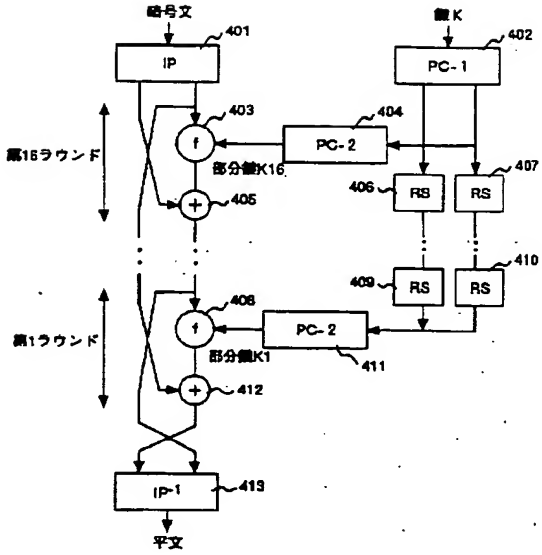
【図3】

図 3



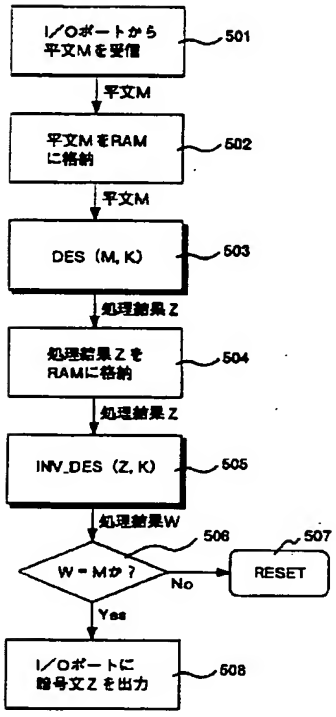
【図4】

図 4



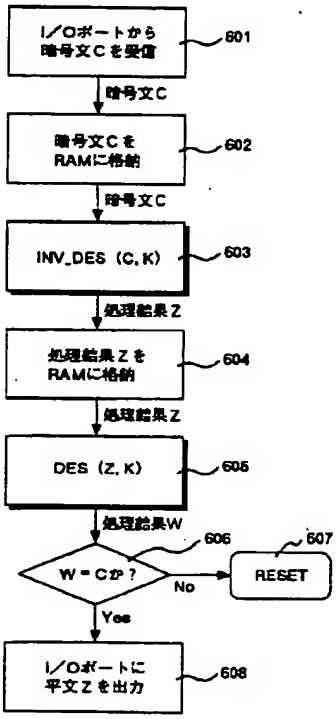
【図5】

図 5



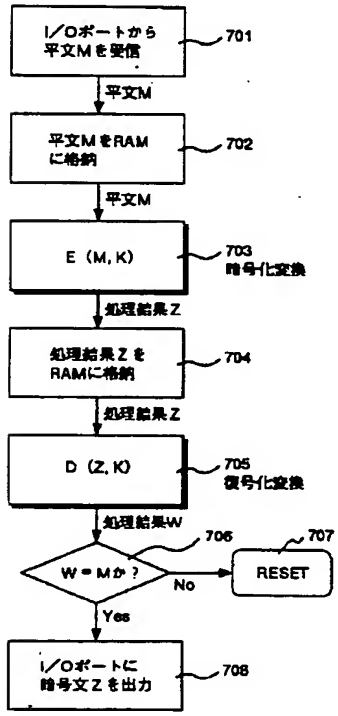
【図6】

図 6



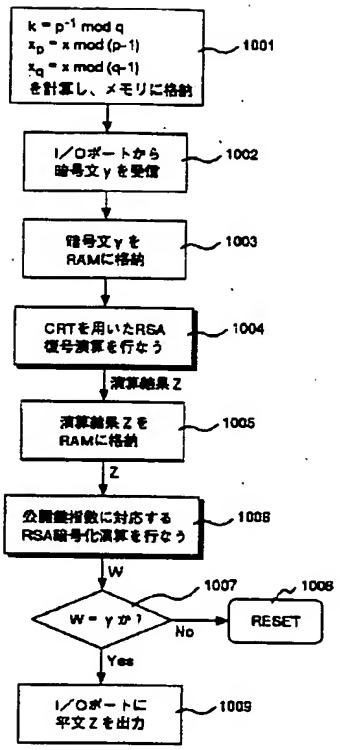
【図7】

図 7



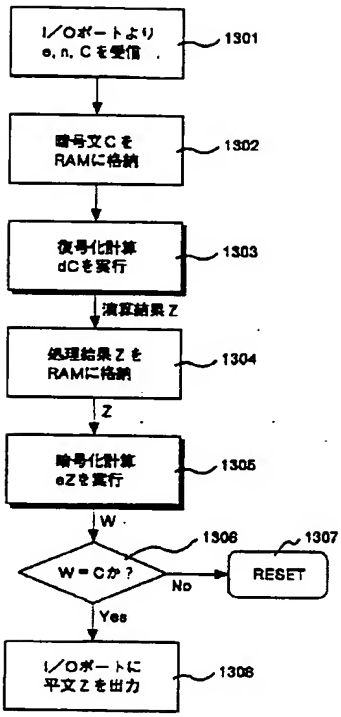
【図１０】

図　１０



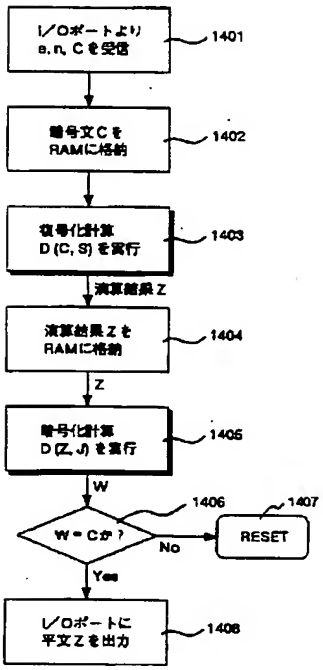
【図１３】

図　１３



【図１４】

図　１４



フロント ページの続き

(72)発明者　渡邊　高志
東京都国分寺市東恋ヶ窪一丁目280番地
株式会社日立製作所中央研究所内

(72)発明者　大木　優
東京都国分寺市東恋ヶ窪一丁目280番地
株式会社日立製作所中央研究所内

Ｆターム(参考)　5B035 AA13 BB09 CA11 CA33 CA38
5J104 JA13 JA28 NA02 NA35 NA40
NA42